



# FortiAnalyzer VM - Install Guide

VERSION 5.4

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



April 11, 2017

FortiAnalyzer VM 5.4 Install Guide

05-540-309958-20170411

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
FortiAnalyzer documentation	6
<b>License and System Requirements</b>	<b>7</b>
Licensing	7
Evaluation license	7
Minimum system requirements	8
<b>Registration and Deployment</b>	<b>9</b>
Register with Customer Service & Support	9
Deployment package	11
Deployment package contents	12
Deploying the appliance	13
<b>Citrix XenServer deployment example</b>	<b>14</b>
Create the virtual machine	14
Configure hardware settings	15
Start the virtual machine	17
<b>Hyper-V deployment example</b>	<b>18</b>
Create the virtual machine	18
Configure hardware settings	19
Start the virtual machine	23
<b>KVM deployment example</b>	<b>24</b>
Create the virtual machine	24
Configure hardware settings	26
Start the virtual machine	27
<b>Open Xen deployment example</b>	<b>28</b>
Create and configure the virtual machine	28
<b>VMware deployment example</b>	<b>31</b>
VMware vSphere	31
Deploy the OVF file	31
Configure hardware settings	34
Power on the virtual machine	35
<b>Azure deployment example</b>	<b>37</b>
Deploy the virtual machine	37

<b>AWS deployment example</b>	<b>39</b>
AWS Marketplace 1-Click Launch	39
AWS EC2 console	41
<b>Initial Configuration</b>	<b>46</b>
GUI access	46
Enable GUI access	46
Connect to the GUI	47
Upload the license file	47
Configure your FortiAnalyzer VM	48
<b>Index</b>	<b>49</b>

## Change Log

Date	Change Description
2016-03-17	Initial release.
2016-06-29	Microsoft Azure instructions added. 32bit VM images removed in 5.4.1.
2016-09-06	Updated VM-BASE storage capacity to 500GB.
2016-09-16	AWS default password information updated.
2017-03-28	Minimum system requirements added.
2017-04-11	KVM storage cache mode updated to <i>writethrough</i> .

# Introduction

The FortiAnalyzer platforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout your network. The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine-tune your policies. Organizations of any size will benefit from centralized security event logging, forensic research, reporting, content archiving, data mining and malicious file quarantining.

FortiAnalyzer offers enterprise class features to identify threats, while providing the flexibility to evolve along with your ever-changing network. FortiAnalyzer can generate highly customized reports for your business requirements, while aggregating logs in a hierarchical, tiered logging topology.

This document describes how to deploy a FortiAnalyzer virtual appliance in several virtualization server environments. This includes how to configure the virtual hardware settings of the virtual appliance. This guide presumes that the reader has a thorough understanding of virtualization servers.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started. For that information, see the *FortiAnalyzer Administration Guide* in the [Fortinet Document Library](#).

## FortiAnalyzer documentation

The following FortiAnalyzer product documentation is available:

- ***FortiAnalyzer Administration Guide***  
This document describes how to set up the FortiAnalyzer system and use it with supported Fortinet units.
- ***FortiAnalyzer device QuickStart Guides***  
These documents are included with your FortiAnalyzer system package. Use these document to install and begin working with the FortiAnalyzer system and GUI.
- ***FortiAnalyzer Online Help***  
You can get online help from the FortiAnalyzer GUI. FortiAnalyzer online help contains detailed procedures for using the GUI to configure and manage devices.
- ***FortiAnalyzer CLI Reference***  
This document describes how to use the FortiAnalyzer Command Line Interface (CLI) and contains references for all CLI commands.
- ***FortiAnalyzer Release Notes***  
This document describes new features and enhancements in the FortiAnalyzer system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.
- ***FortiAnalyzer VM Install Guide***  
This document, which describes installing FortiAnalyzer VM in your virtual environment.

# License and System Requirements

## Licensing

Fortinet offers the FortiAnalyzer VM in a stackable license model. This model allows you to expand your VM solution as your environment expands. For information on purchasing a FortiAnalyzer VM license, contact your Fortinet Authorized Reseller, or visit [http://www.fortinet.com/how\\_to\\_buy/](http://www.fortinet.com/how_to_buy/).

When configuring your FortiAnalyzer VM, ensure to configure hardware settings as outlined in the following table and consider future expansion. Contact your Fortinet Authorized Reseller for more information.

	GB / Day of logs	Storage Capacity
VM-BASE	1	500GB
VM-GB1	+1	+500GB
VM-GB5	+5	+3TB
VM-GB25	+25	+10TB
VM-GB100	+100	+24TB
VM-GB500	+500	+48TB
VM-GB2000	+2000	+100TB

For more information, see [Minimum system requirements on page 8](#), and the FortiAnalyzer product data sheet:

<http://www.fortinet.com/sites/default/files/productdatasheets/FortiAnalyzer-VM.pdf>.

After placing an order for FortiAnalyzer VM, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the FortiAnalyzer VM with Customer Service & Support at <https://support.fortinet.com>.

Upon registration, you can download the license file. You will need this file to activate your FortiAnalyzer VM. You can configure basic network settings from the CLI to complete the deployment. Once the license file is uploaded and validated, the CLI and GUI will be fully functional.

## Evaluation license

FortiAnalyzer VM includes a free, full featured 15 day trial license. No activation is required for the built-in evaluation license.

The trial period begins the first time you start the FortiAnalyzer VM. When the trial expires, all functionality is disabled until you upload a license file.



Technical support is not included with the 15-day evaluation.



Contact your Fortinet Reseller to request a full evaluation (60-days) license.

## Minimum system requirements

The following table lists the minimum system requirements for your VM hardware, based on the number of logs, the log rate, and the number of devices, VDOMs, or ADOMs that your VM manages.

Analytic Sustained Rate (logs/sec)	GB/Day of Logs	Maximum Devices / VDOMs / ADOMs	VM Hardware Requirements		
			RAM (GB)	CPU cores	IOPS
500	75	200	8	2	100
4000	300	2000	16	6	300
7500	500	2000	32	6	600
35000	1600	4000	64	16	1500
48000	4000	10000	64	16	2000
60000	5000	10000	128	24	2500



The collector sustained rate can be calculated by multiplying the analytic sustained rate by 1.5.



This table does not take into account other hardware specifications, such as bus speed, CPU model, or storage type.



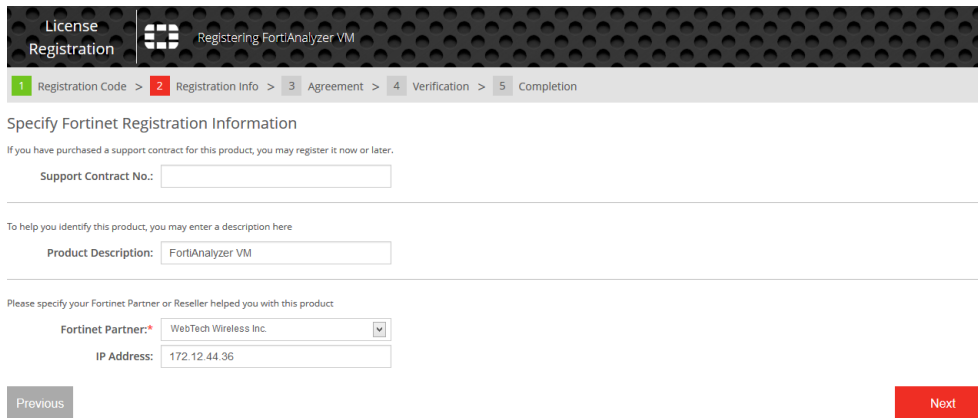
# Registration and Deployment

## Register with Customer Service & Support

To obtain the FortiAnalyzer VM license file you must first register your FortiAnalyzer VM with [Fortinet Customer Service & Support](#).

### To register your FortiAnalyzer VM:

1. Log in to the Fortinet Customer Service & Support portal using an existing support account or click *Create an Account* to create a new account.
2. In the toolbar select *Asset > Register/Renew*. The *Registration Wizard* opens.
3. Enter the registration code from the FortiAnalyzer VM License Certificate that was emailed to you, select the end user type, and then click *Next*. The *Registration Info* page is displayed.



The screenshot shows the 'Registration Info' step of the 'Registering FortiAnalyzer VM' wizard. The progress bar at the top indicates the current step is '2 Registration Info'. The page title is 'License Registration'. Below the progress bar, there are three sections for input: 'Specify Fortinet Registration Information' with a 'Support Contract No.' field; 'To help you identify this product, you may enter a description here' with a 'Product Description' field containing 'FortiAnalyzer VM'; and 'Please specify your Fortinet Partner or Reseller helped you with this product' with a 'Fortinet Partner' dropdown menu (showing 'WebTech Wireless Inc.') and an 'IP Address' field (showing '172.12.44.36'). At the bottom, there are 'Previous' and 'Next' buttons.

4. Enter your support contract number, product description, Fortinet Partner, and IP address in the requisite fields, then select *Next*.



As a part of the license validation process FortiAnalyzer VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiAnalyzer VM's IP address has been changed, the FortiAnalyzer VM must be rebooted in order for the system to validate the change and operate with a valid license.



The [Customer Service & Support](#) portal currently does not support IPv6 for FortiAnalyzer VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

5. On the *Fortinet Product Registration Agreement* page, select the checkbox to indicate that you have read, understood, and accepted the service contract, then select *Next* to continue to the *Verification* page.
6. The verification page displays the product entitlement. Select the checkbox to indicate that you accept the terms then select *Confirm* to submit the request.

7. From the *Registration Completed* page you can download the FortiAnalyzer VM license file, select *Register More* to register another FortiAnalyzer VM, or select *Finish* to complete the registration process.

Select *License File Download* to save the license file (.lic) to your management computer. See [Upload the license file on page 47](#) for instructions on uploading the license file to your FortiAnalyzer VM via the GUI.

#### To edit the FortiAnalyzer VM IP address:

1. In the toolbar select *Asset > Manage/View Products* to open the *View Products* page.
2. Select the FortiAnalyzer VM serial number to open the *Product Details* page.
3. Select *Edit* to change the description, partner information, and IP address of your FortiAnalyzer VM from the *Edit Product Info* page.

4. Enter the new IP address then select *Save*.



You can change the IP address five (5) times on a regular FortiAnalyzer VM license. There is no restriction on a full evaluation license.

5. Select *License File Download* to save the license file (.lic) to your management computer. See [Upload the license file on page 47](#) for instructions on uploading the license file to your FortiAnalyzer VM via the GUI.

## Deployment package

FortiAnalyzer VM deployment packages are included with firmware images on the [Customer Service & Support site](#). The following table list the available VM deployment packages.

VM Platform	Deployment File
Amazon Web Service AMI, EC2, and EBS	The 64bit Amazon Machine Image (AMI) is available in the AWS marketplace.
Microsoft Azure	The Microsoft Azure based VM is available in the Azure portal.
Citrix XenServer 6.2	FAZ_VM64_XEN-v5-buildxxxx-FORTINET.out-.CitrixXen.zip
Linux KVM RedHat 6.5	FAZ_VM64_KVM-v5-buildxxxx-FORTINET.out-.kvm.zip
Microsoft Hyper-V Server 2008 R2 and 2012	FAZ_VM64_HV-v5-buildxxxx-FORTINET.out-.hyperv.zip
Open Source XenServer 4.2.5	FAZ_VM64_XEN-v5-buildxxxx-FORTINET.out-.OpenXen.zip
VMware ESX 4.0 and 4.1 VMware ESXi 4.0, 4.1, 5.0, 5.1, 5.5, and 6.0	ESX/ESXi server: FAZ_VM64-v5-buildxxxx-FORTINET.out.ovf.zip

For more information see the FortiAnalyzer VM datasheet available on the Fortinet web site:

<https://www.fortinet.com/products/management/fortianalyzer.html>.

Firmware image FTP directories are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the FAZ\_VM64\_HV-v5-buildxxxx-FORTINET.out.hyperv.zip image, found in the 5.4.0 directory, is specific to the 64bit Microsoft Hyper-V Server virtualization environment.



You can download the *FortiAnalyzer Release Notes* and MIB file from this directory. The Fortinet Core MIB file is located in the main FortiAnalyzer 5.00 directory.



Download the .out file to upgrade your existing FortiAnalyzer VM installation.

**To download the firmware package:**

1. Log in to the Fortinet Customer Service & Support portal then, from the toolbar select *Download > Firmware Images*. The *Firmware Images* page opens.
2. Select *FortiAnalyzer* from the *Select Product* drop-down list, then select *Download*.
3. Browse to the appropriate directory for the version that you would like to download.
4. Download the appropriate firmware image and release notes to your management computer.
5. Extract the contents of the package to a new folder on your management computer.

## Deployment package contents

**Citrix XenServer**

The `.out.CitrixXen.zip` file contains:

- `faz.xva`: The Citrix XenServer Virtual Appliance (XVA) binary file containing virtual hardware configuration settings.
- `ovf` folder:
  - `FortiAnalyzer.ovf`: Open Virtualization Format (OVF) template file, containing virtual hardware settings for Xen.
  - `faz.vhd`: The FortiAnalyzer VM system hard disk in VHD format.
  - `datadrive.vhd`: The FortiAnalyzer VM log disk in VHD format.

**Linux KVM**

The `.out.kvm.zip` file contains:

- `faz.qcow2`: The FortiAnalyzer VM system hard disk in QCOW2 format.  
The log disk and virtual hardware settings have to be configured manually.

**Microsoft Hyper-V**

The `.out.hyperv.zip` file contains:

- `faz.vhd`: The FortiAnalyzer VM system hard disk in VHD format.  
The log disk and virtual hardware settings have to be configured manually.

**Open Source XenServer**

The `.out.OpenXen.zip` file contains:

- `faz.qcow2`: The FortiAnalyzer VM system hard disk in QCOW2 format.  
The log disk and virtual hardware settings have to be configured manually.

**VMware**

The `.out.ovf.zip` file contains:

- `faz.vmdk`: The FortiAnalyzer VM system hard disk in Virtual Machine Disk (VMDK) format.
- `FortiAnalyzer-VM64.ovf`: The VMware virtual hardware configuration file.
- `DATADRIVE.vmdk`: The FortiAnalyzer VM log disk in VMDK format

## Deploying the appliance

Prior to deploying the FortiAnalyzer VM, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiAnalyzer VM presume that you are familiar with the management software and terminology of your VM platform.

For assistance in deploying FortiAnalyzer VM, refer to the deployment chapter in this guide that corresponds to your hypervisor environment. You may also need to refer to the documentation provided with your VM server. The deployment chapters are presented as examples because, for any particular VM server, there are multiple ways of creating a virtual machine - command line tools, APIs, alternative graphical user interface tools.

Before you start your FortiAnalyzer VM appliance for the first time, you might need to adjust virtual disk sizes and networking settings. With the exception of AWS and Azure environments, the first time you start FortiAnalyzer VM, you will have access only through the console window of your VM server environment. After you configure one network interface with an IP address and administrative access, you can access the FortiAnalyzer GUI (see [GUI access on page 46](#)).

If the FortiAnalyzer VM does not have a valid Logical Volume Management (LVM) configuration, the LVM service will not start automatically upon boot-up when the disk already contains data. To manually enable the service, use the `execute lvm start` CLI command.

# Citrix XenServer deployment example

Once you have downloaded the `FAZ_VM64_XEN-v5-buildxxxx-FORTINET.out.CitrixXen.zip` file and extracted the files, you can create the virtual machine in your Citrix Xen environment.

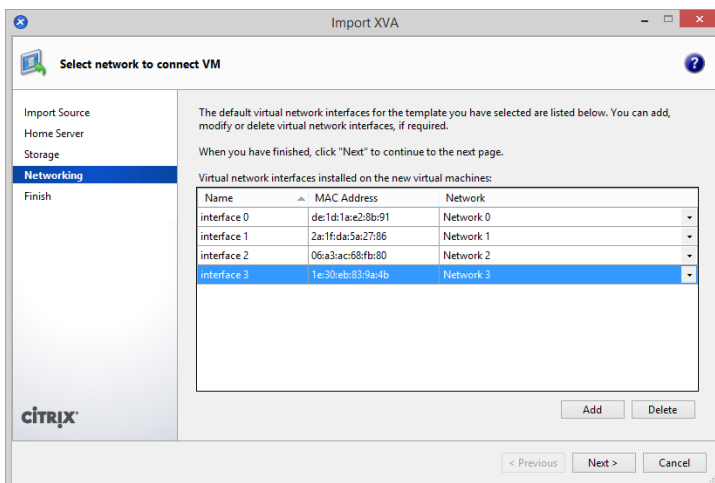
The following topics are included in this section:

- [Create the virtual machine](#)
- [Configure hardware settings](#)
- [Start the virtual machine](#)

## Create the virtual machine

To create the virtual machine:

1. Launch XenCenter on your management computer.  
The management computer can be any computer that can run Citrix XenServer, a Microsoft Windows application.
2. Click **ADD a server**, then enter the Citrix XenServer IP address and the root logon credentials required to manage that server.  
Your Citrix XenServer is added to the list in the left pane, and the *Virtual Machine Manager* home page opens.
3. Select **File > Import**.
4. Click **Browse**, locate the `faz.xva` file, select **Open**, then select **Next**.
5. Choose the pool or standalone server that will host the VM, then click **Next**.
6. Select the storage location for the FortiAnalyzer VM disk drives, then click **Next**.
7. Configure the virtual network interfaces, then click **Next**. By default, there are four virtual network interfaces.



8. Review the import settings, deselect **Start VM(s) after import**, and then click **Finish** to import the VM.

The Citrix XenServer imports the FortiAnalyzer VM files and configures the VM as specified in the template. Depending on your computer's hardware speed and resource load, as well as on the file size and speed of the network connection, this may take several minutes to complete.

When the VM import is complete, the XenServer left pane will include the FortiAnalyzer VM in the list of deployed VMs for your Citrix XenServer.

## Configure hardware settings

Before starting your FortiAnalyzer VM for the first time, you must adjust the VM's virtual hardware settings to meet your network requirements.

To access VM settings, open XenCenter and select the FortiAnalyzer VM in the left pane. The tabs in the right pane provide access to the virtual hardware configuration, and the console tab provides access to the FortiAnalyzer console.

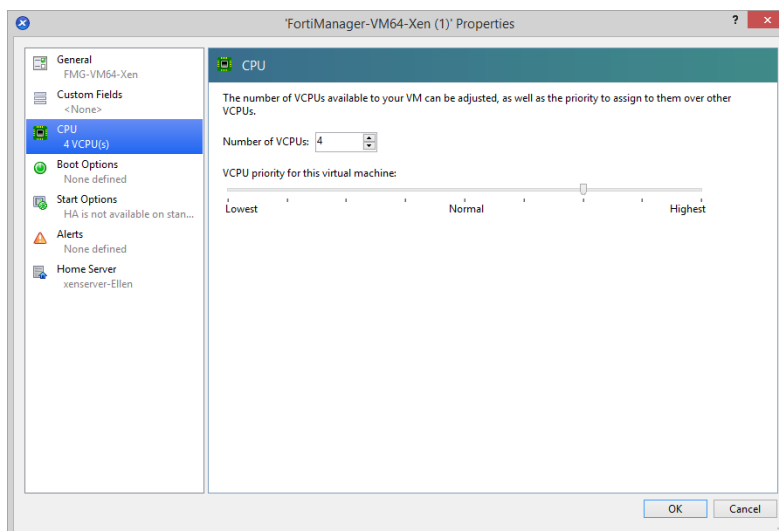


Disk resizing must be done before you start the VM for the first time.

If you know your environment will expand in the future, it is recommended to add hard disks larger than the 500GB base license requirement. This will allow your environment to be expanded as required while not taking up more space than is needed. See [Licensing on page 7](#) for more information.

### To set the number of CPUs:

1. In the XenCenter left pane, right-click the FortiAnalyzer VM and select *Properties*.
2. In the left pane of the *Properties* window, select *CPU*.

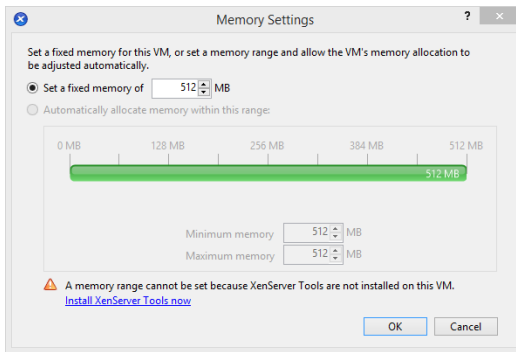


3. Adjust the in the *Number of VCPUs*, then click *OK*.

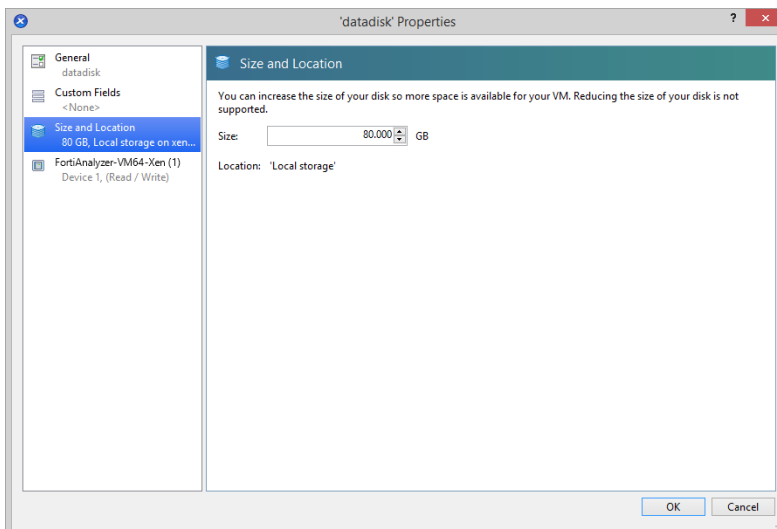
XenCenter will display a warning if you select more CPUs than the Xen host computer contains. Such a configuration might reduce performance.

**To set the memory size:**

1. In the XenCenter left pane, select the FortiAnalyzer VM.
2. In the right pane, select the *Memory* tab.
3. Click *Edit* and modify the value in the *Set a fixed memory of* field. See [Minimum system requirements on page 8](#) to determine your required memory.
4. Click *OK*.

**To resize the data disk:**

1. In the XenCenter left pane, select the FortiAnalyzer VM.
2. In the right pane, select the *Storage* tab.
3. Select the data disk, then click *Properties* to open the *Properties* window.
4. Select *Size and Location*.



5. Adjust the *Size* to the required value, then click *OK*. See [Licensing on page 7](#) for more information.



The FortiAnalyzer VM allows for 12 virtual log disks to be added to a deployed instance. When adding additional hard disks use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```



## Start the virtual machine

You can now proceed to start on your FortiAnalyzer VM.

- In the XenCenter left pane, right-click on the name of the FortiAnalyzer VM and select *Start*.
- Select the name of the FortiAnalyzer VM from the left pane, then select *Start* in the toolbar.

# Hyper-V deployment example

Once you have downloaded the `FAZ_VM64_HV-v5-buildxxxx-FORTINET.out.hyperv.zip` file and extracted the package contents to a folder on your Microsoft server, you can deploy the VHD package to your Microsoft Hyper-V environment.

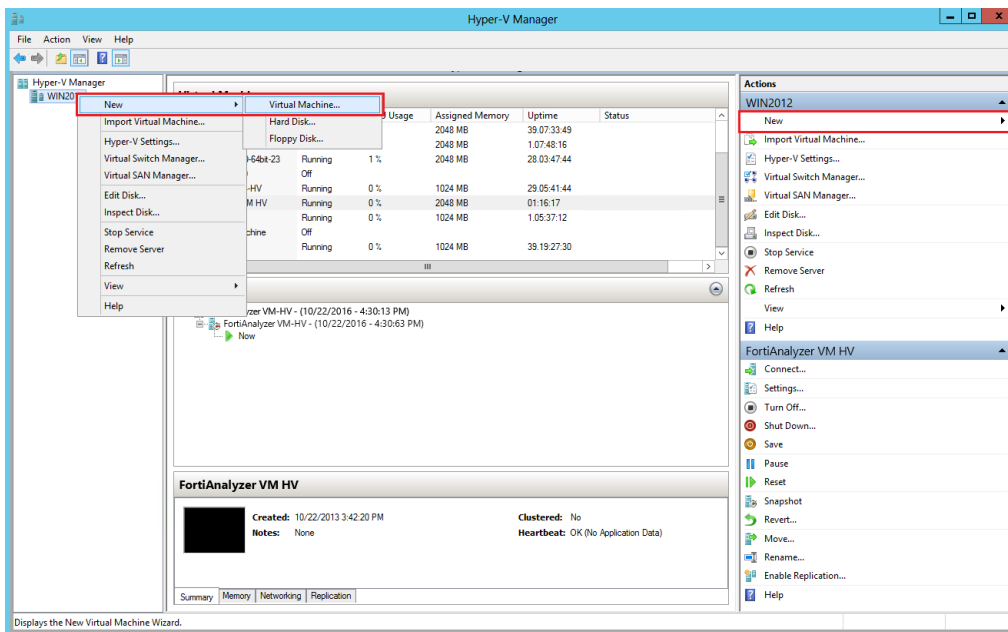
The following topics are included in this section:

- Create the virtual machine
- Configure hardware settings
- Start the virtual machine

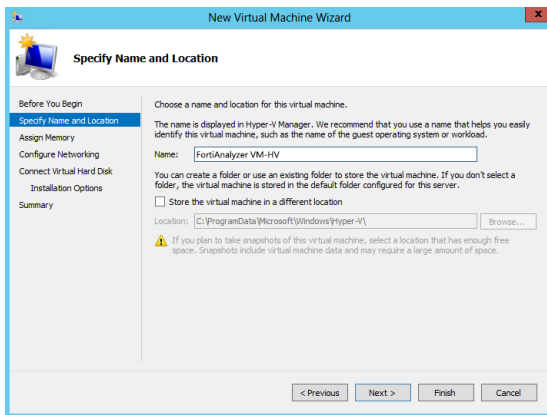
## Create the virtual machine

To create the virtual machine:

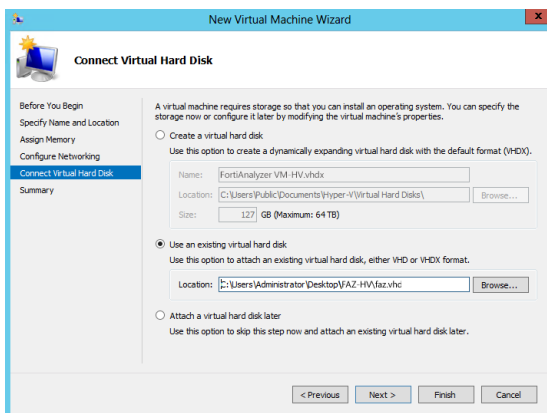
1. Launch the Hyper-V Manager in your Microsoft server. The *Hyper-V Manager* home page opens.
2. Select the server in the right-tree menu. The server details page opens.



3. Right-click the server and select *New > Virtual Machine*, or in the *Actions* menu, select *New > Virtual Machine*. The *New Virtual Machine Wizard* opens.
4. Click *Next* to create a virtual machine with a custom configuration. The *Specify Name and Location* page opens.



5. Enter a name for this VM. The name is displayed in the Hyper-V Manager.
6. Click *Next* to continue to the *Assign Memory* page .
7. Specify the amount of memory to allocate to this virtual machine. See [Minimum system requirements on page 8](#) to determine your required memory.
8. Click *Next* to continue to the *Configure Networking* page.
9. You must configure network adapters in the *Settings* page.  
Each new VM includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. FortiAnalyzer VM requires four network adapters.
10. Select *Next* to continue to the *Connect Virtual Hard Disk* page.

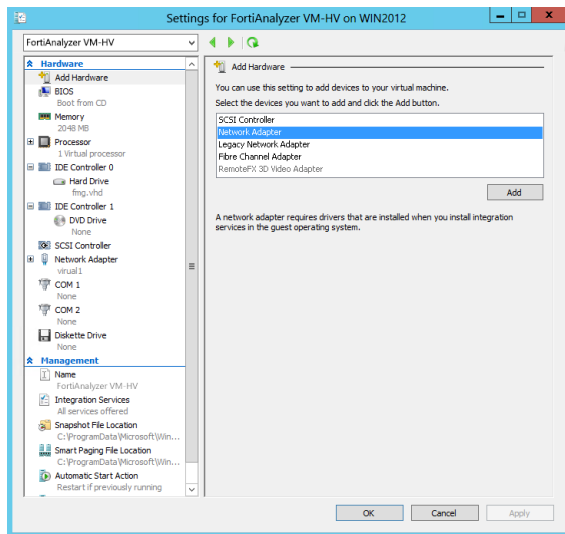


11. Select to use an existing virtual hard disk and browse for the `faz.vhd` file that you downloaded from the [Fortinet Customer Service & Support](#) portal.
12. Select *Next* to continue to the *Summary* page.
13. To create the virtual machine and close the wizard, select *Finish*.

## Configure hardware settings

Before powering on your FortiAnalyzer VM you must configure the virtual processors, memory, network adapters, and hard disk to match your FortiAnalyzer VM license. See [Licensing on page 7](#) for FortiAnalyzer VM license information.

To open the *Settings* page, in the Hyper-V Manager, right-click on the name of the virtual machine and select *Settings*, or select the virtual machine then click *Settings* from the *Actions* menu.

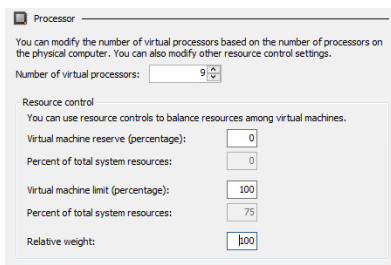


### To configure virtual memory:

1. In the *Settings* page, select *Memory* from the *Hardware* menu. The *Memory* page is displayed.
2. Configure the memory for the VM. See [Minimum system requirements on page 8](#) to determine your required memory.
3. Click *Apply* to save your settings.

### To configure virtual processors:

1. In the *Settings* page, select *Processor* from the *Hardware* menu. The *Processor* page is displayed.



2. Configure the number of virtual processors for the VM. Optionally, you can use resource controls to balance resources among VMs.
3. Click *Apply* to save your settings.

### To configure network adapters:

1. In the *Settings* page, select *Add Hardware* from the *Hardware* menu.
2. From the device list, select *Network Adapter*, then click *Add*. The *Network Adapter* page opens.

**Network Adapter**

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: Broadcom NetXtreme Gigabit Ethernet - Virtual Switch

VLAN ID

☐ Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

☐ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

Remove

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

3. Manually configure four network adapters in the settings page. For each network adapter, select a virtual switch from the drop-down list.
4. Click *Apply* to save your settings.

### To configure the virtual hard disk:



The FortiAnalyzer VM requires at least two virtual hard disks. Before powering on the FortiAnalyzer VM, you must add at least one more virtual hard disk. The default hard drive, `faz.vhd`, contains the operating system. The second hard drive is used for logs.



If you know your environment will expand in the future, it is recommended to add hard disks larger than the 500GB base license requirement. This will allow your environment to be expanded as required while not taking up more space in the Storage Area Network (SAN) than is needed. See [Licensing on page 7](#) for more information.



The FortiAnalyzer VM allows for 12 virtual log disks to be added to a deployed instance. When adding additional hard disks use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```

1. In the *Settings* page, select *IDE Controller 0* from the *Hardware* menu.
2. Select the type of drive that you want to attach to the controller, then click *Add*. The *Hard Drive* page opens.

**Hard Drive**

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 0 Location: 0 (n use)

Media

You can compact or convert a virtual hard disk by editing the associated file. Specify the full path to the file.

☒ Virtual hard disk

C:\Users\Administrator\Desktop\FMG-HV\fmv.vhd

New Edit Inspect Browse...

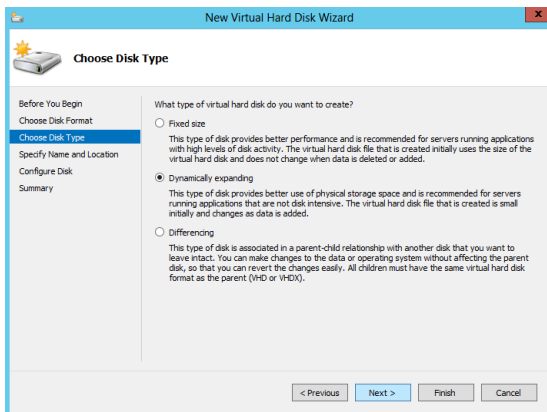
☐ Physical hard disk

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

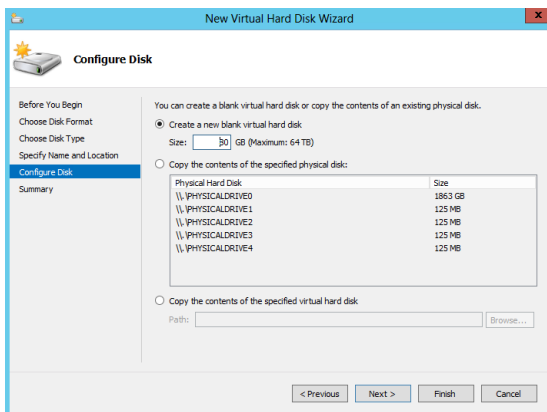
To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

Remove

3. Click *New* to create a new virtual hard disk. The *New Virtual Hard Disk Wizard* opens to help you create a new virtual hard disk.
4. Click *Next* to continue to the *Choose Disk Format* page.
5. Select to use VHDX format virtual hard disks. This format supports virtual disks up to 64TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012.
6. Click *Next* to continue to the *Choose Disk Type* page.



7. Select the type of virtual disk you want to use, one of the following:
  - **Fixed Size:** This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.
  - **Dynamically Expanding:** This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual disk file that is created is small initially and changes as data is added.
  - **Differencing:** This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).
8. Click *Next* to continue to the *Specify Name and Location* page.
9. Specify the name and location of the virtual hard disk file. Use the *Browse* button to select a specific file folder on your server.
10. Click *Next* to continue to the *Configure Disk* page.

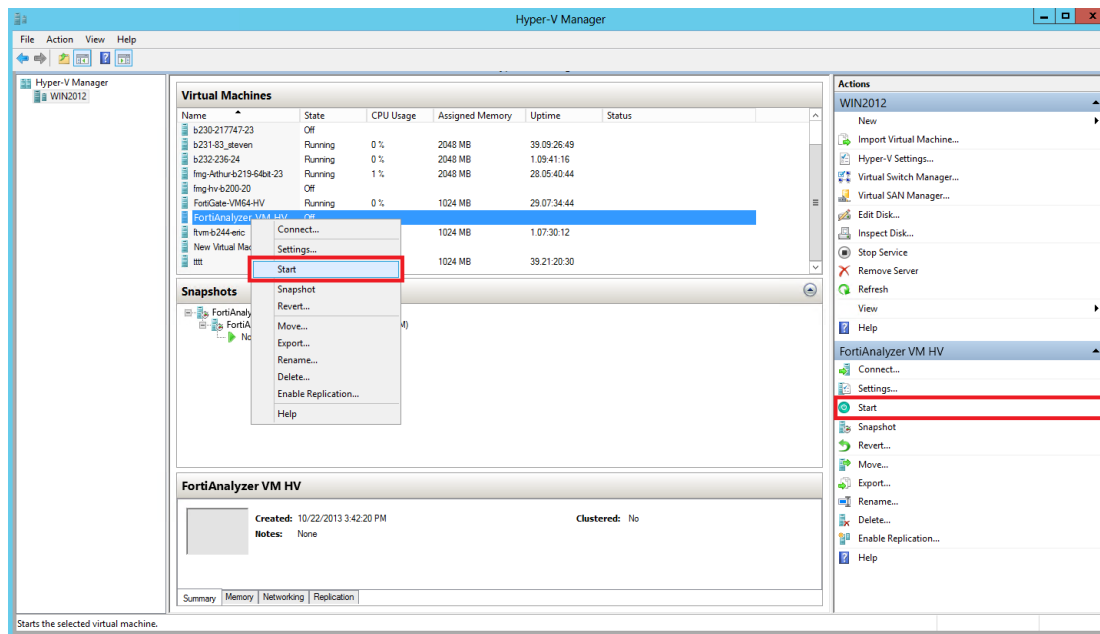


11. Select *Create a new blank virtual hard disk*, then enter the size of the disk in GB. The maximum size is dependent on your server environment.
12. Click *Next* to continue to the *Summary* page.  
The summary page provides details about the virtual hard disk.
13. Click *Finish* to create the virtual hard disk, then click *Apply* to save the settings, and then click *OK* to exit the settings page.

## Start the virtual machine

You can now proceed to power on your FortiAnalyzer VM.

- In the list of virtual machines, right-click on the name of the FortiAnalyzer VM and select *Start*.
- Select the name of the FortiAnalyzer VM from the list of virtual machines, then click *Start* from the *Actions* menu.



# KVM deployment example

Once you have downloaded the `FAZ_VM64_KVM-v5-buildxxxx-FORTINET.out.kvm.zip` file and extracted the virtual hard drive image file, you can create the virtual machine in your KVM environment.

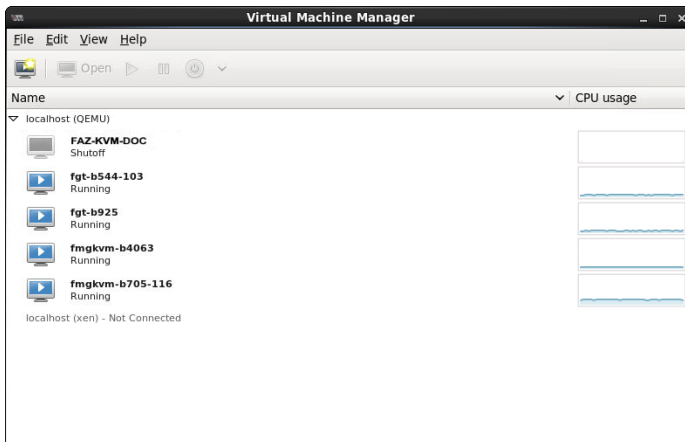
The following topics are included in this section:

- [Create the virtual machine](#)
- [Configure hardware settings](#)
- [Start the virtual machine](#)

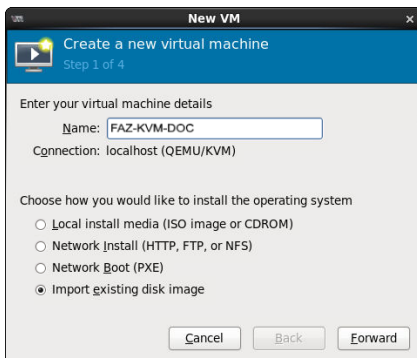
## Create the virtual machine

To create the virtual machine:

1. Launch Virtual Machine Manager (virt-manager) on your KVM host server. The *Virtual Machine Manager* home page opens.

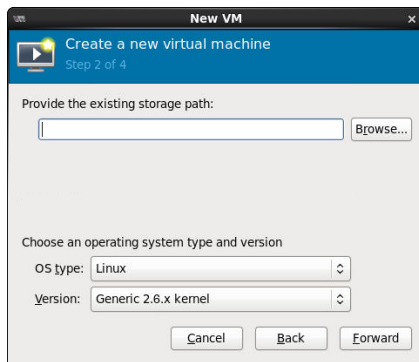


2. Select *Create a new virtual machine* from the toolbar..

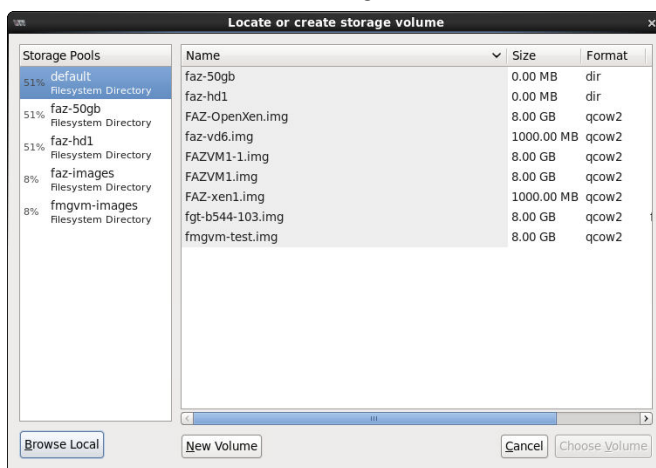


3. Enter a name for the virtual machine, such as *FAZ-KVM-DOC*.
4. Ensure that *Connection* is *localhost*, select *Import existing disk image*, then click *Forward* to continue.

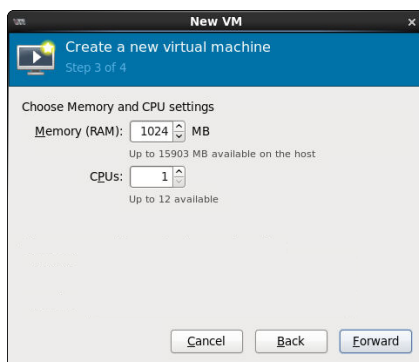




5. In the *OS Type* field select *Linux*.
6. In the *Version* field select *Generic 2.6.x kernel*. You may have to first select *Show all OS options*.
7. Click *Browse* to locate the storage volume.



8. If you copied the *faz.qcow2* file to */var/lib/libvirt/images* it will be shown on the right. If you saved it elsewhere on the server, click *Browse Local* to find it.
9. Once the file has been located, click *Choose Volume*, then click *Forward*.



10. Specify the amount of memory and the number of CPUs to allocated to this VM, then select *Forward*. See [Minimum system requirements on page 8](#) to determine your required memory.
11. Expand the *Advanced options* section. By default, a new virtual machine includes one network adapter. Select a network adapter on the host computer.  
Optionally, set a specific MAC address for the virtual network interface.

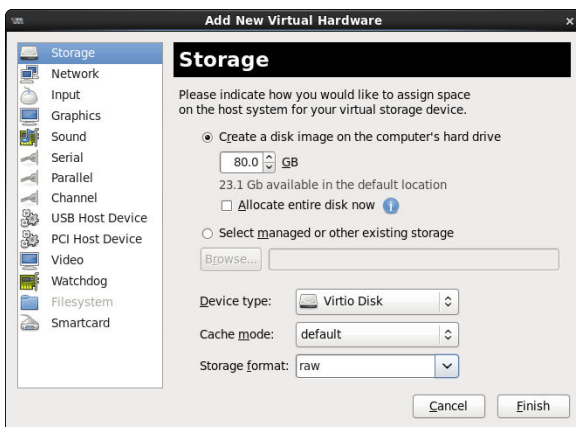
12. Set *Virt Type* to *virtio* and set *Architecture* to *qcow2*.
13. Click *Finish* to create the VM.

## Configure hardware settings

Before powering on your FortiAnalyzer VM you must configure virtual disks and at least four network interfaces.

### To configure settings on the server:

1. In the Virtual Machine Manager, locate the name of the VM, then select *Open* from toolbar.
2. In the Virtual Machine window, select *Show virtual hardware details*.
3. Click *Add Hardware* to open the *Add Hardware* window
4. Select *Storage*.



5. Select *Create a disk image on the computer's harddrive*, and set the size to 80GB.



If you know your environment will expand in the future, or if you will be using ADOMs, it is recommended to add hard disks larger than 500GB. This will allow your environment to be expanded as required while not taking up more space than is needed. See [Licensing on page 7](#) for more information.



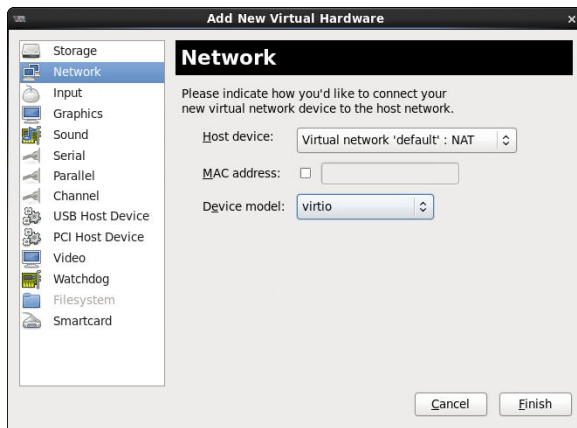
The FortiAnalyzer VM allows for 12 virtual log disks to be added to a deployed instance. When adding additional hard disks use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```

6. Enter the following information:

<b>Device Type</b>	Virtio disk
<b>Cache mode</b>	writethrough
<b>Storage format</b>	raw

7. Select *Network* to add more network interfaces. The *Device Model* must be *Virtio*.



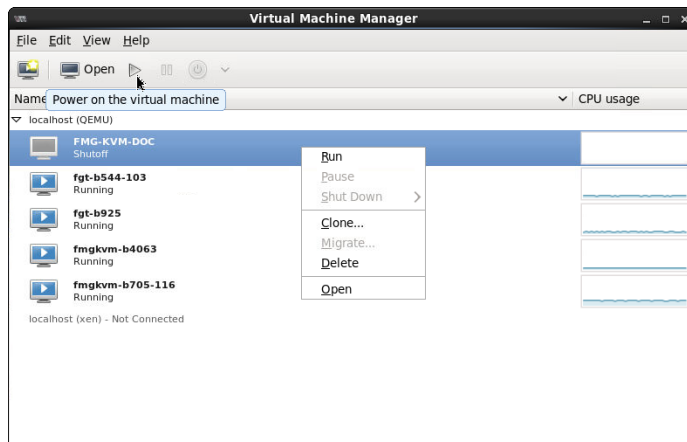
A new VM includes one network adapter by default. More can be added through the *Add Hardware* window. FortiAnalyzer VM supports up to four network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.

8. Click *Finish*.

## Start the virtual machine

You can now proceed to power on your FortiAnalyzer VM.

- Right-click on the FortiAnalyzer VM and select *Run*, or
- Select the FortiAnalyzer VM from the list of VMs, then click *Power on the virtual machine* from the toolbar.



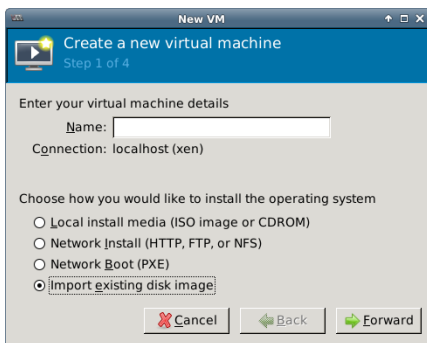
# Open Xen deployment example

Once you have downloaded the `FAZ_VM64_XEN-v5-buildxxxx-FORTINET.out.OpenXen.zip` file and extracted the `faz.qcow2`, you can create the virtual machine in your Open Xen environment.

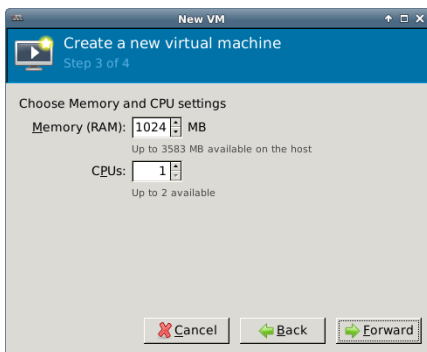
## Create and configure the virtual machine

To deploy and configure the virtual machine:

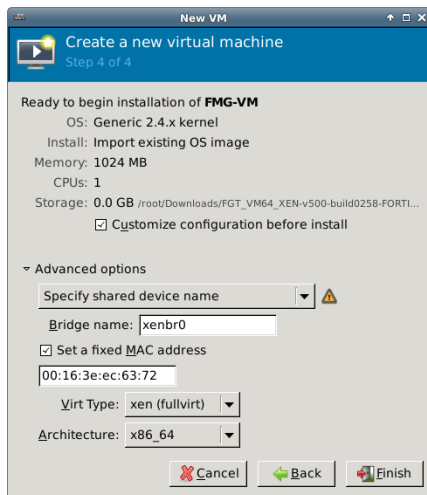
1. Launch Virtual Machine Manager (virt-manager) on your Open Xen host server. The *Virtual Machine Manager* home page opens.
2. Select *Create a new virtual machine* from the toolbar..



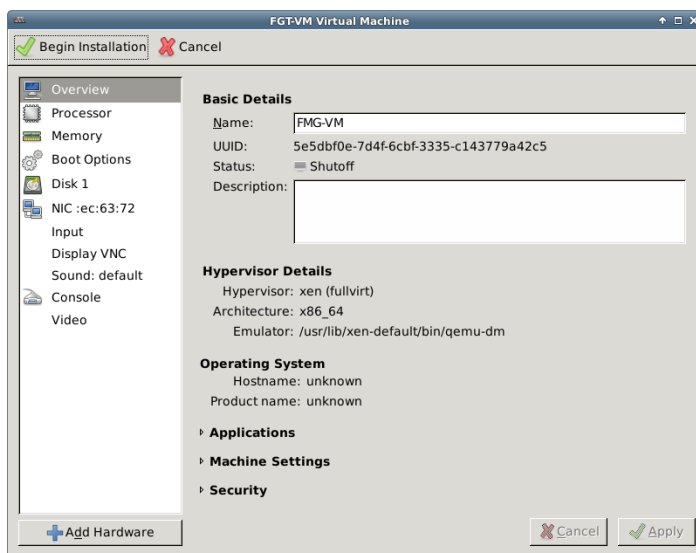
3. Enter a name for the VM, such as *FAZ-VM*.
4. Ensure that *Connection* is *localhost*, select *Import existing disk image*, then click *Forward* to continue.
5. In the *OS Type* field select *Linux*. In the *Version* field select *Generic 2.6.x kernel*.
6. Click *Browse* to open the *Locate or create storage volume* window.
7. Click *Browse Local*, find the `faz.qcow2` disk image file, then click *Choose Volume* and then *Forward*.



8. Specify the amount of memory and the number of CPUs to allocated to this VM. See [Minimum system requirements on page 8](#) to determine your required memory.
9. Click *Forward*.



10. Select *Customize configuration before install*. This enables you to make hardware configuration changes before the VM creation is started.
11. Expand the *Advanced options* section.
  - By default, a new virtual machine includes one network adapter.
  - Select *Specify shared device name*, and enter the name of the bridge interface on the Open Xen host.
  - Optionally, set a fixed MAC address for the virtual network interface.
  - *Virt Type* and *Architecture* are set by default and should not need to be changed.
12. Click *Finish*. The virtual machine hardware configuration window opens. It can be used to add hardware such as network interfaces and disk drives.



13. Click *Add Hardware* to open the *Add Hardware* window, then click *Storage*.
14. Select *Create a disk image on the computer's hddrive*, and set the size to an appropriate size.



If you know your environment will expand in the future, or if you will be using ADOMs, it is recommended to add hard disks larger than 500GB. This will allow your environment to be expanded as required while not taking up more space than is needed. See [Licensing on page 7](#) for more information.



The FortiAnalyzer VM allows for 12 virtual log disks to be added to a deployed instance. When adding additional hard disks use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```

---

- 15.** Select *Network* to add more network interfaces.

A new VM includes one network adapter by default. More can be added through the *Add Hardware* window. FortiAnalyzer VM required four network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.

- 16.** Click *Finish*.

- 17.** Click *Begin Installation*.

After the installation completes successfully, the VM will start and the console window will open.

# VMware deployment example

The FortiAnalyzer VM can be deployed and configured using VMware vSphere Hypervisor™ (ESX/ESXi) and VMware vSphere Client™.

## VMware vSphere

Once you have downloaded the `FAZ_VM64-v5-buildxxxx-FORTINET.out.ovf.zip` file and extracted the package contents to a folder on your management computer, you can deploy the OVF package to your VMware environment.

Prior to deploying the FortiAnalyzer VM, ensure that the following are configured and functioning properly:

- VMware vSphere Hypervisor™ (ESX/ESXi) software must be installed on a server and updated to the latest patch release prior to installing FortiAnalyzer VM. Go to <http://www.vmware.com/products/vsphere-hypervisor/index.html> for installation details.
- VMware vSphere Client™ must be installed on the computer that you will be using for managing the FortiAnalyzer VM.

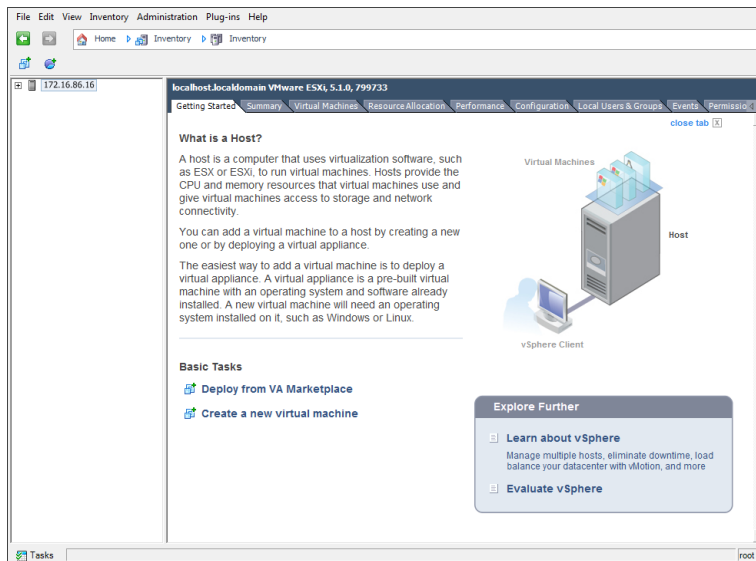
The following topics are included in this section:

- [Deploy the OVF file](#)
- [Configure hardware settings](#)
- [Power on the virtual machine](#)

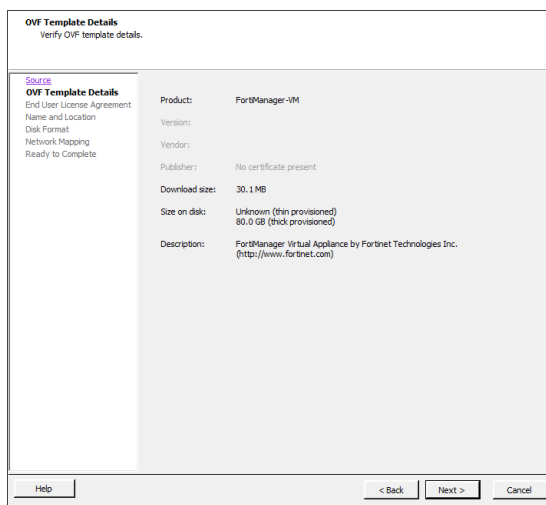
## Deploy the OVF file

**To deploy the OVF file template:**

1. Launch the VMware vSphere client, enter the IP address or host name of your server, enter your user name and password, then click *Login*. The vSphere client home page opens.



2. Select **File > Deploy OVF Template** to launch the OVF Template wizard. The OVF Template *Source* page opens.
3. Click **Browse**, locate the OVF file on your computer, then click **Next** to continue. The OVF Template *Details* page opens.



4. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Click **Next** to continue. The OVF Template *End User License Agreement* page opens.
5. Read the end user license agreement, then click **Accept** then **Next** to continue. The OVF Template *Name and Location* page opens.
6. Enter a name for this OVF template. The name can contain up to 80 characters and it must be unique within the inventory folder. Click **Next** to continue. The OVF Template *Disk Format* page opens.



7. Select one of the following:

- **Thick Provision Lazy Zeroed:** Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
- **Thick Provision Eager Zeroed:** Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
- **Thin Provision:** Allocates the disk space only when a write occurs to a block, but the total volume size is reported by the Virtual Machine File System (VMFS) to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains in the volume regardless of if you have deleted data, etc.



If you know your environment will expand in the future, it is recommended to add hard disks larger than the FortiAnalyzer VM base license requirement and utilize *Thin Provision* when setting the OVF Template disk format. This will allow your environment to be expanded as required while not taking up more space in the SAN than is needed.

8. Click *Next* to continue. The OVF Template *Network Mapping* page opens.

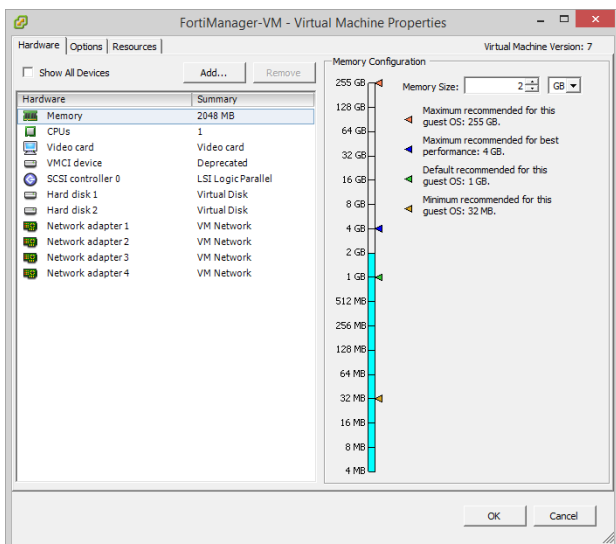
9. Map the networks used in this OVF template to networks in your inventory. Network 1 maps to port1 of the FortiAnalyzer VM. You must set the destination network for this entry to access the device console. Click *Next* to continue. The OVF Template *Ready to Complete* page opens.
10. Review the template configuration.  
Ensure that *Power on after deployment* is not enabled. You might need to configure the FortiAnalyzer VM hardware settings prior to powering on the VM.
11. Click *Finish* to deploy the OVF template. You will receive a *Deployment Completed Successfully* dialog box once the FortiAnalyzer VM OVF template wizard has finished.

## Configure hardware settings

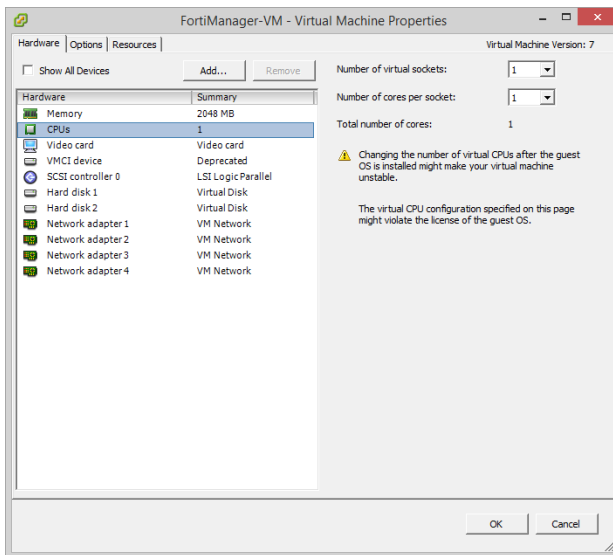
Before powering on your FortiAnalyzer VM you must configure the virtual memory, virtual CPU, and virtual disk.

### To configure the VM:

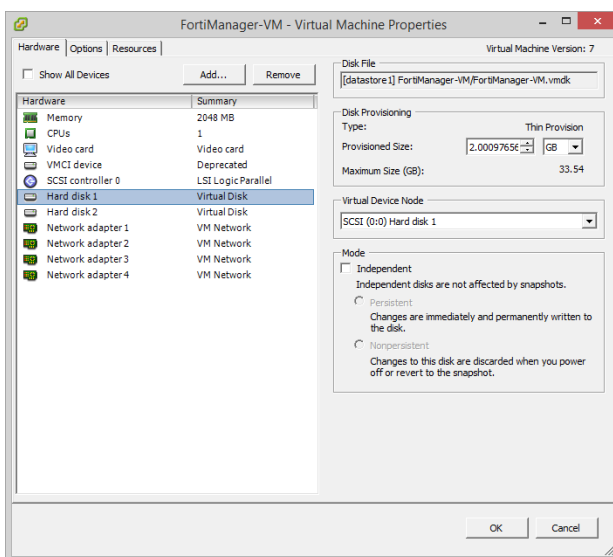
1. In the vSphere Client, right-click on the FortiAnalyzer VM in the left pane and select *Edit Settings* to open the *Virtual Machine Properties* window.
2. Select *Memory* from the *Hardware* list, then adjust the *Memory Size* as required. See [Minimum system requirements on page 8](#) to determine your required memory.



3. Select *CPUs* from the *Hardware* list, then adjust the *Number of virtual sockets* and *Number of cores per socket* as required.



4. Select *Hard disk 2*, the log disk, from the *Hardware* list, and configure it as required. *Hard disk 1* should not be edited.



The FortiAnalyzer VM allows for 12 virtual log disks to be added to a deployed instance. When adding additional hard disks use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg >>
```

5. Click *OK* to apply your changes.

## Power on the virtual machine

You can now proceed to power on your FortiAnalyzer VM.

- Select the FortiAnalyzer VM in the left pane and click *Power on the virtual machine* in the *Getting Started* tab.
- Select the VM in the left pane, then click *Power On* in the toolbar.
- Right-click the VM in the left pane, then select *Power > Power On* from the right-click menu.

# Azure deployment example

FortiAnalyzer VM can be deployed on Microsoft Azure. Prior to deploying the VM, the following are required:

- Microsoft Azure subscription
- Virtual network
- Storage account

## Deploy the virtual machine

This section shows the steps for deploying the FortiAnalyzer VM from your Microsoft Azure dashboard.

### To deploy the VM:

1. Log in to your Azure account.
2. Click *New* in the option pane
3. Enter *FortiAnalyzer* in the search field on the *New* blade, then click *Fortinet FortiAnalyzer for Azure* in the results list.
4. In the FortiAnalyzer VM blade, confirm that the deployment model is correct, then click *Create*.
5. Fill out the basic configuration settings:

<b>VM Name</b>	Enter a name for the virtual appliance.
<b>Administrative Username</b>	Enter the administrative name for the VM. It cannot be <code>admin</code> .
<b>Password</b>	Enter then confirm the admin account password. The password must be between 6 and 72 characters long, and contain characters from 3 of: uppercase characters, lowercase characters, numbers, and special characters.
<b>Subscription</b>	Optionally, select a subscription from the drop-down list.
<b>Resource Group</b>	Enter a current Resource Group for the VM, or create a new group.
<b>Location</b>	Optionally, select a location from the drop-down list.

6. Click *OK* to proceed to the network and storage setting. Configure the following:

<b>Virtual network</b>	Select a current virtual network, or create a new one.
<b>Subnets</b>	Confirm or customize the subnet for the VM, including: <ul style="list-style-type: none"><li>• Outside Subnet name</li><li>• Outside Subnet address prefix</li><li>• Inside Subnet name</li><li>• Inside Subnet address prefix</li></ul>

<b>Virtual machine size</b>	Select the size of the VM to provision. At least <i>Standard A2</i> , with 3.5GB of RAM and two disks, must be selected.
<b>Storage Account</b>	Select a storage account, or create a new account, to contain the disk drives of the VM.

- Click *OK* to proceed to the IP assignment setting. Configure the following:

<b>Public IP address name</b>	Enter the public IP address name, or create a new one.
<b>Domain name label</b>	Enter the DNS prefix to use for the public IP address.
<b>Public IP Address Type</b>	Select if the IP address is static or dynamic.
<b>Outside Address</b>	Confirm or customize the IP address of the outside interface of the VM.
<b>Inside Address</b>	Confirm or customize the IP address of the inside interface of the VM.

- Click *OK* to proceed to the *Summary* blade. If the VM fails validation, correct the errors and try again. Click *Download template* to download the VM template as a JSON file.
- Click *OK* to open the *Create* blade.
- Read the terms of use and privacy policy, then click *Create* to create the VM.
- To connect to the FortiAnalyzer VM GUI, open a web browser and use the public DNS address as the URL:  
`https://<public DNS address>`
- Log in with the configured administrative username and password to configure your FortiAnalyzer VM.

# AWS deployment example

FortiAnalyzer VM can be deployed on the AWS Elastic Compute Cloud (EC2). Prior to deploying the VM, the following are required:

- Amazon EC2 account

The FortiAnalyzer VM can be deployed using either the AWS Marketplace *1-Click Launch* option, or directly from the EC2 console.

This chapter includes the following sections:

- [AWS Marketplace 1-Click Launch](#)
- [AWS EC2 console](#)

## AWS Marketplace 1-Click Launch

This section shows the steps for deploying the FortiAnalyzer VM from the AWS Marketplace using the *1-Click Launch* option.

**To deploy the VM from the AWS Marketplace:**

1. Log in to AWS.
2. From the AWS Marketplace, find the [Fortinet FortiAnalyzer-VM](#) page by searching with the key word *Fortinet*, or by selecting *Security* in the left pane.
3. On the FortiAnalyzer VM page, click *Continue*.

The screenshot shows the AWS Marketplace interface for the Fortinet FortiManager-VM. At the top, there's a navigation bar with the AWS Marketplace logo, user information (Hello, A Harris), and links to 'Your Account', 'Help', and 'Sell on AWS Marketplace'. Below the navigation bar is a search bar and a 'Shop All Categories' dropdown. The main content area is titled 'Launch on EC2: Fortinet FortiManager-VM'. It features two tabs: '1-Click Launch' (selected) and 'Manual Launch'. The '1-Click Launch' tab contains a section titled 'Click "Accept Terms & Launch with 1-Click" to launch this software with the settings below'. This section lists several configuration options: 'Version' (v5.2.2, released 05/11/2015), 'Region' (US East (N. Virginia)), 'EC2 Instance Type' (m1.medium), 'VPC Settings' (Will launch into: subnet-96f7dfac), 'Security Group' (Updated: Create new security group based on seller settings), and 'Key Pair' (Please create a new key pair). To the right of these settings is a 'Price for your selections:' section. It lists the pricing details: 'Bring Your Own License (BYOL)' (Available for customers with current licenses), '\$0.09 / hour' (m1.medium EC2 Instance usage fees), '\$0.05 / GB / month' (EBS Magnetic Storage), and '\$0.05 / 1 million I/O requests' (EBS Magnetic Storage). Below this is an 'Accept Terms & Launch with 1-Click' button. At the bottom right, there is a 'Cost Estimator' section. It also lists the pricing details: 'Bring Your Own License (BYOL)' (Available for customers with current licenses purchased via other channels), '\$62.64 / month' (plus m1.medium EC2 Instance usage fees), and 'Assumes 24 hour use over 30 days'.

4. Select a region and the instance type. Ensure that the instance type fits the size of your deployment and potential future growth.

**Region**

US West (Oregon) ▼

**EC2 Instance Type**

m1.medium  
m1.large  
m1.xlarge  
hi1.4xlarge  
m3.xlarge  
m3.2xlarge

Memory 3.75 GB  
CPU 2 EC2 Compute Units (1 virtual core with 2 EC2 Compute Units)  
Storage 1 x 410 GB  
Platform 64-bit  
Network performance Moderate  
API Name m1.medium

5. Under **Security Group**, ensure that *Create new based on seller settings* is selected from the drop-down list. The only open port that is required for the initial configuration of the VM is port 443, which will allow for an HTTPS connections to the GUI. The remaining ports can also be opened to allow for all potential FortiAnalyzer communication.

**Security Group**

**Updated:** Due to a change in other settings, security group settings is updated.  
A security group acts as a firewall that controls the traffic allowed to reach one or more instances.  
Learn more about [Security Groups](#).

You can create a new security group based on seller-recommended settings or choose one of your existing groups.

Create new based on seller settings ▼

**Description:**  
A new security group will be generated by AWS Marketplace. It is based on recommended settings for Fortinet FortiManager-VM version v5.0.4 provided by Fortinet Inc.

Connection Method	Protocol	Port Range	Source (IP or Group)
SSH	tcp	22 - 22	Anywhere ▼ 0.0.0.0/0
HTTP	tcp	80 - 80	Anywhere ▼ 0.0.0.0/0
HTTPS	tcp	443 - 443	Custom IP ▼ 10.10.10.10
	tcp	514 - 514	Anywhere ▼ 0.0.0.0/0
	tcp	541 - 541	Anywhere ▼ 0.0.0.0/0
	tcp	2032 - 2032	Anywhere ▼ 0.0.0.0/0
	tcp	3000 - 3000	Anywhere ▼ 0.0.0.0/0
	tcp	5199 - 5199	Anywhere ▼ 0.0.0.0/0
	tcp	6020 - 6020	Anywhere ▼ 0.0.0.0/0
	tcp	6028 - 6028	Anywhere ▼ 0.0.0.0/0
HTTP*	tcp	8080 - 8080	Anywhere ▼ 0.0.0.0/0
	tcp	8890 - 8890	Anywhere ▼ 0.0.0.0/0
DNS	udp	53 - 53	Anywhere ▼ 0.0.0.0/0
	udp	6022 - 6022	Anywhere ▼ 0.0.0.0/0
	udp	6023 - 6023	Anywhere ▼ 0.0.0.0/0
	tcp	8888 - 8888	Anywhere ▼ 0.0.0.0/0

**Warning**  
Rules with source of 0.0.0.0/0 allows all IP addresses to access your instance. We recommend limiting access to only known IP addresses.

6. Use the instructions provided under **Key Pair** to create a new key pair, or use an existing key pair if it is secure.
7. Click **Accept Terms & Launch with 1-Click** to deploy the instance and view the summary page.
8. Close the summary page, then, from the software subscriptions page, click **Manage in AWS Console** to view the VM instance and the public DNS address.



Amazon Web Services Home  
Hello, A Harris. (Sign out) | Your Account | Help | Sell on AWS Marketplace

Shop All Categories | Search AWS Marketplace | GO | Your Software

Your Account > | See all AWS Account Activity

Your Software Subscriptions (1) | Enable and create billing alerts for AWS Marketplace charges

Products	Instances	Actions
<b>Fortinet FortiManager-VM</b> <a href="#">Contact vendor</a> <a href="#">Write a review</a> <a href="#">Cancel subscription</a>	<div>1 active</div> <div>i-fc11ca0b <span>running</span></div> <div>Version v5.4.0</div> <a href="#">Manage in AWS Console</a>   <a href="#">Access Software</a>	<a href="#">Usage Instructions</a> <a href="#">Launch more software</a>

The public DNS address is used to connect to and configure the FortiAnalyzer VM via the GUI.

EC2 Dashboard | Launch Instance | Connect | Actions

search: i-fc11ca0b | Add filter | 1 to 1 of 1

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
	i-fc11ca0b	m1.medium	us-west-2a	running	2/2 checks passed	None	ec2-52-24-115-179.us-w...

Instance: i-fc11ca0b | Public DNS: ec2-52-24-115-179.us-west-2.compute.amazonaws.com

**Description** | Status Checks | Monitoring | Tags | Usage Instructions

Instance ID	Public DNS
i-fc11ca0b	ec2-52-29-115-179.us-west-9.compute.amazonaws.com

**Instance state**: running  
**Instance type**: m1.medium  
**Private DNS**: ip-172-31-29-75.us-west-2.compute.internal  
**Private IPs**: 172.31.29.75  
**Secondary private IPs**:  
**VPC ID**: vpc-2667e143

**Public IP**: 52.29.115.179  
**Elastic IP**: -  
**Availability zone**: us-west-2a  
**Security groups**: Fortinet FortiManager-VM-v5-2-2-AutoGenByAWSMP- view rules  
**Scheduled events**: No scheduled events  
**AMI ID**: FortiManager VM64-AWS build0906 AMI Release-c9d3a2a25-5e65-444b-b91b-3c6d0c2afae6-ami-296d3d40.2 (ami-900090ad)

- To connect to the FortiAnalyzer VM GUI, open a web browser and use the public DNS address as the URL:  
`https://<public DNS address>`
- Log in with default username `admin` and the instance ID as the password to configure your FortiAnalyzer VM.



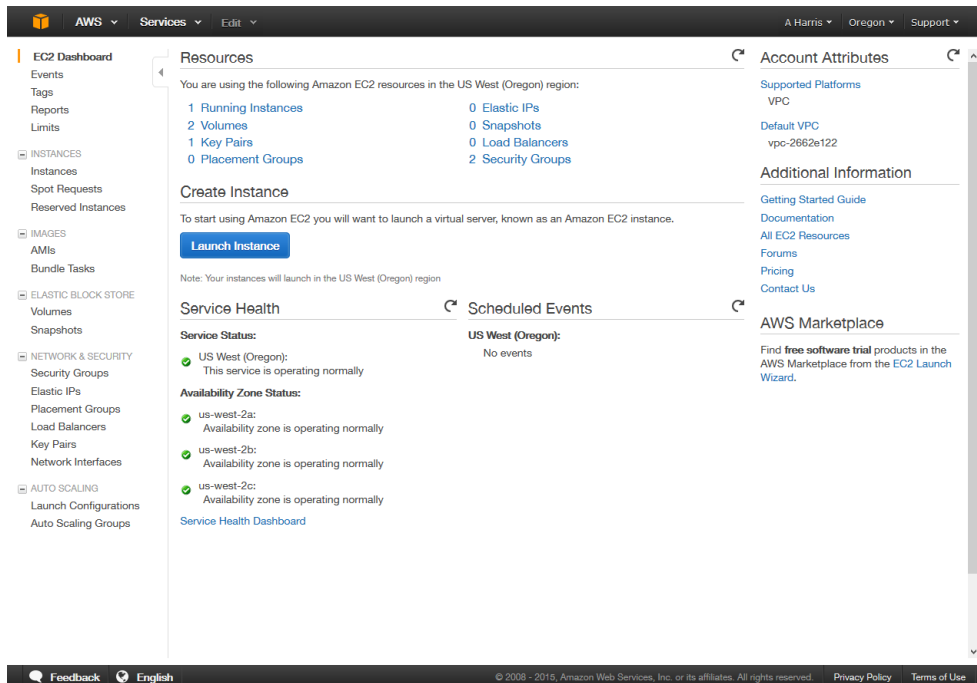
In FortiAnalyzer VM 5.4.1 and earlier, if the instance ID is a long ID (19 characters), only the first 10 characters are used as the default password.

## AWS EC2 console

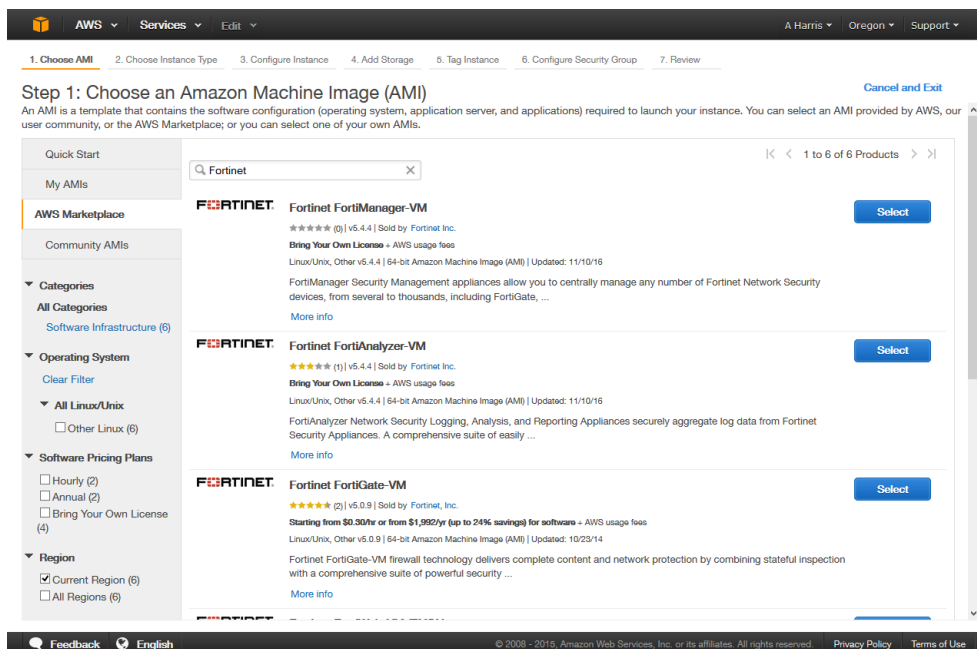
This section shows the steps for deploying the FortiAnalyzer VM directly from the EC2 console.

## To deploy the VM from the EC2 console:

1. Log in to AWS and go to your EC2 dashboard.



2. Click *Launch Instance* to choose an Amazon Machine Image (AMI).  
Select the *AWS Marketplace* category, then search for *Fortinet*.



3. Select the FortiAnalyzer VM, and then choose the instance type that matches your license.

**Step 2: Choose an Instance Type**

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: **General purpose** **All generations** [Show/Hide Columns](#)

Currently selected: m1.medium (2 ECUs, 1 vCPUs, Intel Xeon Family, 3.7 GiB memory, 1 x 410 GiB Storage Capacity)

Note: The vendor recommends using a **m1.medium** instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate
<input checked="" type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input checked="" type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input checked="" type="checkbox"/>	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
<input checked="" type="checkbox"/>	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.xlarge	4	15	2 x 40 (SSD)	Yes	High
<input type="checkbox"/>	General purpose	m3.2xlarge	8	30	2 x 80 (SSD)	Yes	High
<input checked="" type="checkbox"/>	General purpose	m1.small	1	1.7	1 x 160	-	Low
<input checked="" type="checkbox"/>	General purpose	<b>m1.medium</b>	1	3.7	1 x 410	-	Moderate
<input type="checkbox"/>	General purpose	m1.large	2	7.5	2 x 420	Yes	Moderate

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

- Click **Next: Configure Instance Details** to configure the instance details, including the public subnet and network interfaces.

**Step 3: Configure Instance Details**

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances:

Purchasing option: ☐ Request Spot Instances

Network:  [Create new VPC](#)

Subnet:  [Create new subnet](#)

Auto-assign Public IP:

IAM role:  [Create new IAM role](#)

Shutdown behavior:

Enable termination protection: ☐ Protect against accidental termination

Monitoring: ☐ Enable CloudWatch detailed monitoring  
[Additional charges apply.](#)

Tenancy:   
[Additional charges will apply for dedicated tenancy.](#)

**Network interfaces**

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	<a href="#">New network interface</a>	subnet-d579c5a2	Auto-assign	<a href="#">Add IP</a>

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

A network interface must be manually created so that you can upload your license file. Up to two interfaces can be attached to the instance.

- Click **Next: Add Storage** to configure the instance's storage based on your requirements.

**Step 4: Add Storage**

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/sda	snap-ac081f90	1	Magnetic	N/A	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensitive)	10	Magnetic	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

**General Purpose (SSD)** volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB. [Set my root volume to General Purpose \(SSD\)](#).

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Tag Instance](#)

- Click **Next: Tag Instance** to create a tag. A tag consists of a key-value pair. It is useful to create tags to quickly reference instance items in your deployment. Up to 10 tags can be added.

**Step 5: Tag Instance**

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
Name	FortManager VM
Public IP	10.0.0.3
Private IP	10.0.1.3

[Create Tag](#) (Up to 10 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

- Click **Next: Configure Security Group**, then either create a new security group, or select an existing security group. The default provided security group is based on recommended settings the FortiAnalyzer VM.

**Step 6: Configure Security Group**

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group  
☐ Select an existing security group

Security group name: FortinetFortManager-VM-v5.2.2-AutoGenByAWSMP-1

Description: This security group was generated by AWS Marketplace and is based on recommen

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere 0.0.0.0/0
HTTP	TCP	80	Anywhere 0.0.0.0/0
HTTPS	TCP	443	Anywhere 0.0.0.0/0
Custom TCP Rule	TCP	514	Anywhere 0.0.0.0/0
Custom TCP Rule	TCP	541	Anywhere 0.0.0.0/0
Custom TCP Rule	TCP	2032	Anywhere 0.0.0.0/0
Custom TCP Rule	TCP	3000	Anywhere 0.0.0.0/0
Custom TCP Rule	TCP	5199	Anywhere 0.0.0.0/0
Custom TCP Rule	TCP	6020	Anywhere 0.0.0.0/0
Custom TCP Rule	TCP	6028	Anywhere 0.0.0.0/0
Custom TCP Rule	TCP	8080	Anywhere 0.0.0.0/0
Custom TCP Rule	TCP	8890	Anywhere 0.0.0.0/0
DNS (UDP)	UDP	53	Anywhere 0.0.0.0/0
Custom UDP Rule	UDP	6022	Anywhere 0.0.0.0/0
Custom UDP Rule	UDP	6023	Anywhere 0.0.0.0/0
Custom TCP Rule	TCP	8888	Anywhere 0.0.0.0/0

Add Rule

**Warning**  
 Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Previous **Review and Launch**

- Click **Review and Launch**. If necessary, decide which boot volume to boot the instance from.
- Review the instance, including the AMI details, instance type, security groups, instance details, storage, and tags. Edit the configuration as needed.
- Click **Launch**, select **Proceed without a key pair** from the drop-down list, then select the checkbox acknowledging that you already have the username and password for the AMI.

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Proceed without a key pair

☒ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

Cancel Launch Instances

- Click **Launch Instances** to launch the new FortiAnalyzer VM instance.
- To connect to the FortiAnalyzer VM GUI, open a web browser and use the public DNS address as the URL:  
`https://<public DNS address>`
- Log in with default username `admin` and the instance ID as the password to configure your FortiAnalyzer VM.



In FortiAnalyzer VM 5.4.1 and earlier, if the instance ID is a long ID (19 characters), only the first 10 characters are used as the default password.

# Initial Configuration

Before you can connect to the FortiAnalyzer VM you must configure basic configuration via the CLI console. Once configured, you can connect to the FortiAnalyzer VM GUI and upload the FortiAnalyzer VM license file that you downloaded from the [Customer Service & Support](#) portal.

The following topics are included in this section:

- [GUI access](#)
- [Upload the license file](#)
- [Configure your FortiAnalyzer VM](#)

## GUI access



FortiAnalyzer VM AWS and Azure instances do not require any special configuration to enable GUI access. The GUI can be accessed with the public DNS

## Enable GUI access

To enable GUI access to the FortiAnalyzer VM you must configure the port1 IP address and network mask of the FortiAnalyzer VM.

**To configure the port1 IP address and netmask:**

1. In your hypervisor manager, start the FortiAnalyzer VM and access the console window. You might need to press *Enter* to see the login prompt.

```
File Edit View Inventory Administration Plug-ins Help
172.16.86.16
FortiGate-VM179
FortiGate-VM32-171
FortiGate-VM32-171-1
FortiGate-VM32-171-2
FortiGate-VM32-171-4
FortiGate-VM32-171-8
FortiGate-VM64
FortiGate-VM64-171
FortiGate-VM64-171-02
FortiGate-VM64-171-2
FortiGate-VM64-171-4
FortiGate-VM64-171-8
FortiGate-VM64-178
FortiGate-VM64-179
FortiGate-VM64-656
FortiManager-VM-01
Windows
Tasks root

FortiManager-VM-01
Getting Started Summary Resource Allocation Performance Events Console Permissions

EXTLINUX 3.53 2007-11-17 EBIOS Copyright (C) 1994-2007 H. Peter Anvin
Loading vmlinuz...
Loading /rootfs.gz...
.....ready.
Creating LVM volume ... done
Formatting LVM disk (ext4)... done
Creating swapfile...OK

Initialize file systems...
New version: v5.8-build0151 130320 (GA Patch 2)

FMG-UMB4 login: GUI started.
FMG-UMB4 login: admin
Password:
FMG-UMB4 # _
```

2. At the FortiAnalyzer VM login prompt, enter the username *admin*, then press *Enter*. By default, there is no password.
3. Using CLI commands, configure the port1 IP address and netmask.

For example:

```
config system interface
  edit port1
    set ip <IP address> <Netmask>
  end
```



You can also use the *append allowaccess* command to enable other access protocols, such as *auto-ipsec* and *snmp*. The *ping*, *https*, *ssh*, and *fgfm* protocols are enabled by default.

For more information, see the *FortiAnalyzer CLI Reference* in the [Fortinet Document Library](#).



The port management interface should match the first network adapter and virtual switch that you have configured in the hypervisor virtual machine settings.

4. To configure the default gateway, enter the following commands:

```
config system route
  edit 1
    set device port1
    set gateway <gateway_ipv4_address>
  end
```



The Customer Service & Support portal does not currently support IPv6 for FortiAnalyzer VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

## Connect to the GUI

Once you have configured the port1 IP address and network mask, launch a web browser and enter the IP address you configured for the port management interface. At the login page, enter the user name *admin* and no password, then select *Login*.

The GUI will open with an *Evaluation License* dialog box.

## Upload the license file

FortiAnalyzer VM includes a free, full featured 15 day trial.

Before using the FortiAnalyzer VM you must enter the license file that you downloaded from the [Customer Service & Support](#) portal upon registration.

**To upload the license via the CLI:**

1. Open the license file in a text editor and copy the VM license string.
2. In a FortiAnalyzer VM console window, enter the following:

```
execute add-vm-license <"vm license string">
```

See the [FortiAnalyzer CLI Reference](#), available from the [Fortinet Document Library](#), for more details on using this command.

**To upload the license file via the GUI:**

1. In the *Evaluation License* dialog box, select *Enter License*.  
Optionally, you can also select *Upload License* in the *License Information* dashboard widget.
2. In the license upload page, click *Browse*, locate the VM license file (.lic) on your computer, then click *OK* to upload the license file.  
A reboot message will be shown, then the FortiAnalyzer VM system will reboot and load the license file.
3. Refresh your browser and log back into the FortiAnalyzer VM with username *admin* and no password.  
The VM registration status appears as valid in the *License Information* widget once the license has been validated.



As a part of the license validation process FortiAnalyzer VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiAnalyzer's IP address has been changed, the FortiAnalyzer VM must be rebooted in order for the system to validate the change and operate with a valid license.

If the IP address in the license file and the IP address configured in the FortiAnalyzer VM do not match, you will receive an error message when you log back into the VM.

If this occurs, you will need to change the IP address in the [Customer Service & Support](#) portal to match the management IP and re-download the license file. To change the management IP address, see [To edit the FortiAnalyzer VM IP address: on page 10](#)



After an invalid license file has been loaded onto the FortiAnalyzer VM, the GUI will be locked until a valid license file is uploaded. A new license file can be uploaded via the CLI.

## Configure your FortiAnalyzer VM

Once the FortiAnalyzer VM license has been validated, you can configure your device. For more information on configuring your FortiAnalyzer VM, see the *FortiAnalyzer Administration Guide* available in the [Fortinet Document Library](#).



# Index

---

## A

Amazon Machine Image See AMI

Amazon Web Service See AWS

AMI 11, 42

AWS 5, 11, 13, 39, 41, 46

1-Click Launch 39

Marketplace 39, 42

## C

Citrix 11-12, 14

XenCenter 14-15, 17

XenServer 11-12, 14

CLI 6-7, 13, 16, 21, 26, 30, 35, 46-48

Command Line Interface See CLI

configure

CPU 20

disk 21

hardware 7, 28, 34

memory 16

VM 28, 34, 48

CPU 8, 15, 25, 28, 34

configure 20

cores 8

## D

datasheet 11

deploy 6, 28, 31, 37

OVF 31

---

package 11

VM 37, 39, 42

device

maximum 8

model 11, 26

name 29

type 26

disk

configure 21

resize 15-16

virtio 26

DNS

public 38, 40, 45-46

Domain Name Server See DNS

download

firmware 12

## E

EC2 11, 39, 41

Elastic Compute Cloud See EC2

ESX 11, 31

ESXi 11, 31

## F

firmware 6, 11

download 12

float 33

## G

Graphical User Interface See GUI

GUI

access 46

## H

hardware requirements 8

Hyper-V 11-12, 18, 20

## I

instance 16, 21, 26, 30, 35, 40, 42

    ID 41, 45

interface 13-14, 25-26, 29, 43

IOPS 8

IP address 9, 13-14, 31, 38, 46, 48

## K

KVM 5, 11-12, 24

## L

license 2, 7, 9, 15, 19, 32, 42, 46-48

    evaluation 7, 10, 47-48

    file 7, 9, 43, 46-47

    trial 7

    upload 48

logs

    daily maximum 7-8

## M

MAC 25, 29

map 34

maximum

    devices 8

    logs per day 7-8

Media Access Control See MAC

memory

    configure 16

    minimum 8

    size 16, 19, 25, 28, 34

    virtual 20, 34

minimum

    cores 8

    IOPS 8

    memory 8

## N

network

    adapter 19, 25, 27, 29-30, 47

    interface 13-14, 25-26, 29, 43

    map 34

## O

Open Virtualization Format See OVF

Open Xen 28

OVF 12, 31

    deploy 31

    package 31

    template 31-32

## P

package

    contents 12

    deployment 11

    OVF 31

    VHD 18

password 5, 31, 37, 41, 45, 47-48

pool 14

provision 38

## Q

QCOW2 12

## R

register 7, 9

requirements 8

## S

SAN 21, 33

storage

- account 37-38

- add 43

- format 26

- location 14

- physical 22

- type 8

- volume 25, 28

Storage Area Network See SAN

system requirements 5, 7-8

## V

VHD 12, 18

- package 18

virtio 26

virtual

- memory 20, 34

Virtual Hard Disk See VHD

Virtual Machine See VM

Virtual Machine Disk See VMDK

Virtual Processor See CPU

## VM

- configure 28, 34, 48

- create 14, 18, 24, 26, 28, 38

- deploy 37, 39, 42

- start 17, 23, 27, 35

VMDK 12

VMware 11-12, 31

- vSphere 31, 34

vSphere 31, 34

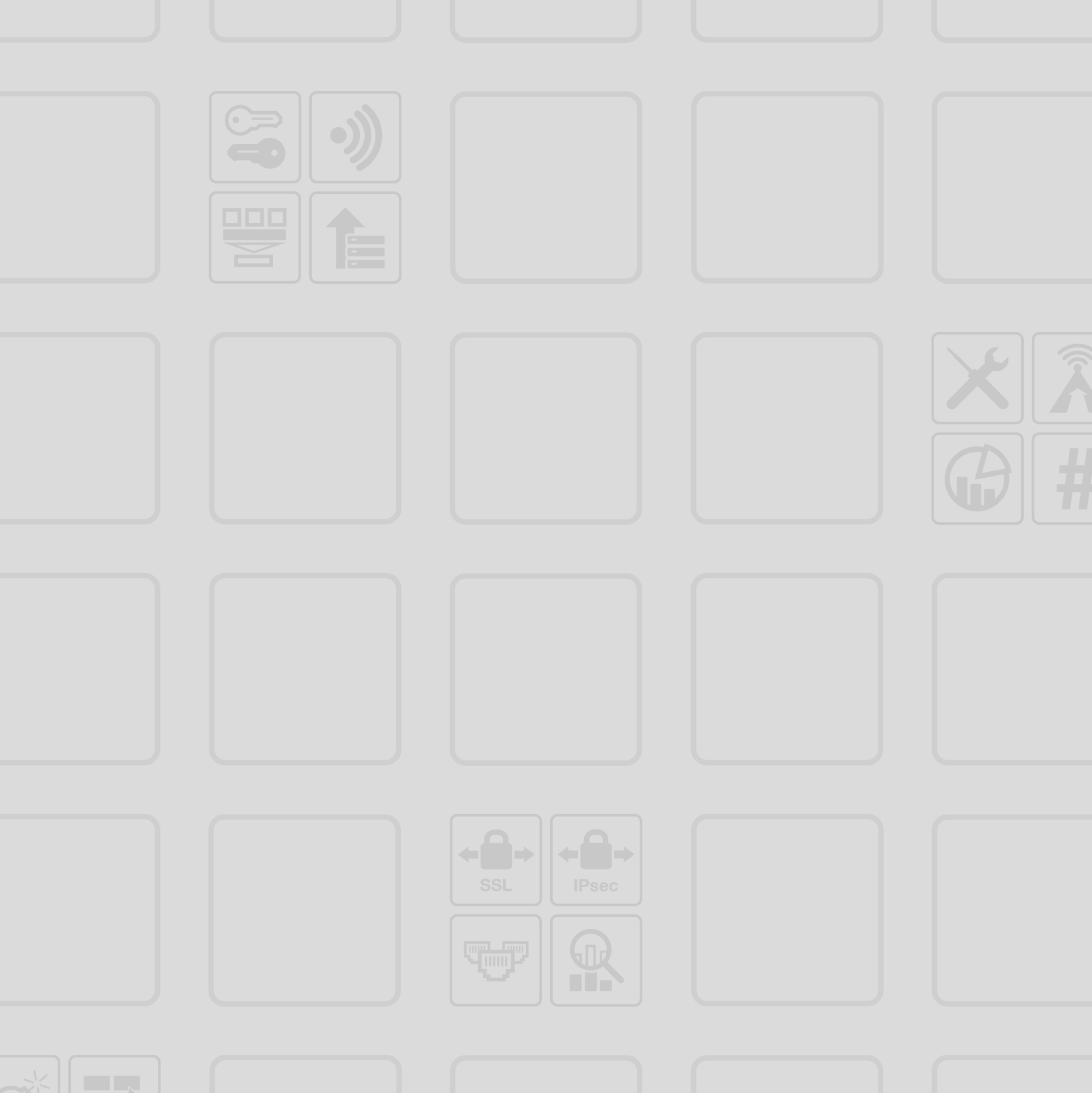
## X

XenCenter 14-15, 17

XenServer 11-12, 14

XenServer Virtual Appliance See XVA

XVA 12



**FORTINET®**

*High Performance Network Security*



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.